

安全协议:信息安全保障的灵魂

——安全协议分析研究现状与发展趋势*

薛锐 雷新锋

(中国科学院软件研究所信息安全国家重点实验室 北京 100190)

摘要 信息社会对于信息保障技术手段提出了极大的挑战。安全协议作为信息安全保障的灵魂,越来越凸显出其关键和纽带作用。对安全协议的安全性分析则是信息时代一个重要而无法回避的关键问题。文章通过总结安全协议分析的研究现状与发展趋势,认为我国目前该领域的研究与国外差距较大,加强协议安全性分析研究对我国来说是一个非常迫切的课题。在此基础上,提出了相关对策与建议。

关键词 安全协议,密码学,形式化方法,研究现状,发展趋势

DOI: 10.3969/j.issn.1000-3045.2011.03.006



中国科学院



薛锐研究员

1 安全协议在信息社会中的重要意义

(1)信息社会中,网络已经成为人类文明飞速发展的主要载体。人类社会目前正经历着自工业革命以来最为深刻的信息革命。

在短短的几十年时间里,信息革命已经经历了单机时期、互联网时期,如今正在走向物联网时期。如果说互联网时期,信息的流动从形式上仅限于虚拟世界,那么物联网的出现就意味着虚拟世界与现实世界的界限将逐步模糊。因此,可以说,在信息社会中,网

络的触角正在延伸至精神世界与物质世界的每一个角落,成为人类文明飞速发展的主要载体。

(2)信息的安全保障问题是信息时代的一个永远无法回避的关键问题。任何事情都有其两面性。网络一方面促进了人类文明的飞速发展,另一方面也成为不同文明、不同利益集团之间相互角逐的战场。在这个战场中,信息的窃取、网络攻击将成为影响力最大、杀伤力最强的武器,大到影响国家的政治、经济、军事、文化等,小到影响个人的日常生活的方方面面。毫无疑问,信息的安全保障问题对信息社会的影响是广泛而深刻的,是这个时代发展中一个无法回避的关键问题。

(3)安全协议是信息安全保障的灵魂。安全协议是通过一系列步骤定义的分布式算法,这些步骤确切规范了两方或多方主体为达到某个安全目标要采取的动作。其目的

* 收稿日期:2011年4月11日

是在网络信道不可靠的情况下,确保通信安全以及传输数据的安全。为了实现不同的信息安全保障,人们需要借助于不同类型的协议来达到相应的目的。具体来说,人们常常要达到的保密性、完整性、可用性、认证性、不可否认性、公平性、匿名性等等都要通过安全协议,使用适当的安全机制加以实现。根据这些安全目的的不同,安全协议通常分为保密协议、密钥建立协议、认证协议、公平交换协议、电子投票协议等。

另一方面,各种安全机制,例如加密、签名、认证码等都是要通过安全协议在实际应用中发挥作用。具体的安全机制通常并不直接面向用户的安全需求,而是通过安全协议来体现的。事实上,所有的信息交换必须在一定的协议规范下完成,并且所有密码手段都将通过安全协议来发挥自己的作用。形象地说来,门锁就像密码机制一样,是保障房间安全的手段,而协议就像门一样,通过将锁安装到门上,实现对于房间的安全保护。协议分析就像分析一把锁在门上安装的位置、方法等等是否合理,来确定其能否达到保护房间的目的。根据采用的安全机制不同,安全协议通常被分为对称加密、非对称加密和签名协议、承诺和零知识证明协议等。

另外,安全协议还是各种安全信息系统之间的纽带。因为在网络的层次结构中,硬件层面,网络是计算机的纽带,在软件层面,协议是信息系统间的纽带,而安全协议是安全信息系统之间的关键和纽带。人们通常将软件比做计算机的灵魂,那么,在网络环境下,安全协议就是信息安全保障的灵魂。没有安全的协议,就没有信息的安全传输和储存,网络信息的安全需求将无法得到满足。可见,对于信息安全保障来说,安全需求是目标,安全机制是手段,网络是载体,安全协

议是关键和灵魂。

上述表明,安全协议在信息社会发挥着极为重要的作用,是信息安全保障的灵魂。因此,协议的安全性必须受到足够的重视。

2 安全协议分析概述

尽管安全协议在信息安全保障中扮演着如此重要的角色,但要判断一个协议是否能够在具有敌手的非安全环境下正确地达到其预定的安全属性却并非易事。例如,Needham 和 Schroeder 曾提出了著名的 Needham-Schroeder 协议,但时隔 17 年,到 1996 年,G. Lowe 使用形式化工具发现了该协议的一个漏洞。造成这个状况的原因,一方面是由于安全协议的分析具有其固有的复杂性,另一方面是由于当时协议分析手法缺乏,主要靠人工经验对于协议进行攻击分析。显然,依赖手工或经验的方法来判断一个协议的安全性是不足取的。要判断协议的安全性,必须依赖于现代计算机的手段和数学模型,采用严格的方法做出令人信服的分析。目前,对安全协议的分析方法大致可分为两类:一类是基于计算复杂性的方法,另一类是形式化方法。

基于计算复杂性的方法也称为计算方法,其主要思路是:将协议的安全性与某些公认的难题关联起来。在安全性证明时,首先假设敌手能够以某种策略成功攻击协议,然后利用这种攻击策略,构造概率多项式时间的一种解决难题的策略。由于解决难题成功的概率被公认是可忽略的,因此攻击协议成功的概率也是可忽略的。这些难题可以是代数或数论中的难题,例如循环群上的离散对数假设,以及 RSA 假设以及大数分解困难假设等;也可以是计算机理论中一般性的难解问题,如单向函数的存在性、伪随机生成器的存在性。这些问题往往没有被确切地证明的确是难解问题,而是被公认为难解问

题,所以称为假设。这些假设从本质上来说与计算机科学中“ $P \neq NP$ ”的假想有千丝万缕的联系。虽然目前对该问题还缺乏证明或否认,但人们大多对此持肯定态度。除了假设外,这种证明过程是严格的,令人信服的,且其证明过程常常包含一些巧妙的设计,体现着科学与艺术的完美组合。遗憾的是利用这种方法对协议的证明只是安全协议分析的一个方面。如果存在一个证明,则可以断言这个协议是安全的。如果找不到这样的证明,则对于协议的设计和改进行没有、或者说少有任何帮助和意义。况且,这种证明的过程往往繁杂难读,极易发生错误。事实说明,甚至一些著名专家的证明过程也难免发生错误,可见这个过程的复杂性不可低估。

形式化方法也称符号化方法,它通过对协议各要素进行符号化抽象,将计算机科学中的各种形式化方法应用于安全协议的分析中。这里面有定理证明的方法和模型检测的方法。其中定理证明方法的主要思路是:假设安全协议中所使用的各种密码方案本身是完善的,即不可破解的;在此基础上,对协议各要素进行抽象化、符号化,同时将协议中所使用的安全机制公理化;最后通过逻辑推理,证明协议的安全性。这种方法基于形式化理论,协议的安全性是通过符号化公式来刻画的,安全性证明中使用了确定的形式化以及完善安全的概念。另一类方法是模型检测的方法,主要原理是:将安全协议的运行表达为适当的模型;同时将协议的安全属性表达为适当的逻辑公式。检测在这个模型中,这个公式是否被满足。这里需要强调的是,在模型的表达中,要增加一个敌手行为的要素。这些要素符合 Dolev-Yao 刻画的敌手的行为模型。利用形式化方法对协议的分析过程有一个较大的优势,就是它可以自动化。如果一个协议存在漏洞,则可以将这

个漏洞明显地表示出来,从而为协议的设计和改进行提供有力的证据。目前一个最大的目标是:通过开发相关的自动验证工具,使得协议的具体分析过程可由非专业人员完成。

以上两种方法的区别是显而易见的。计算方法的分析所给出的安全性结论更为量化,更为具体,可信度更强,但分析过程复杂,不易于自动化,而且许多时候可能根本无法在协议安全性与困难问题之间建立关联;形式化方法分析过程简单,易于自动化,但由于采用了对于协议某些要素的抽象,降低了其分析结果的可信度。

这种形势催生了以上两种方法融合的研究,即计算可靠的形式化方法。其基本思路是:同时建立安全协议的形式化模型和计算模型,然后证明在形式化模型下的安全性可被映射或解释为计算模型下相应的安全性。这样,既保证了证明结果的计算可靠性,又可保持形式化验证的简洁性。这里的计算可靠性的证明是一劳永逸的,只需要在形式化模型建立之初进行证明,之后的使用中只需直接在形式化模型中进行即可。这当然是一种非常好的思路,但在具体实施中还有很多问题需要解决。一个本质的问题在于,这种形式化模型的抽象程度如何把握。一个抽象程度低的方案可给出更具体的安全结论,但往往会使得协议的安全性不可判定,使其难以自动化,而抽象程度高的形式化模型又往往会使得一些安全隐患被忽视。

随着全球信息化程度的不断深化,安全协议分析面临越来越严峻的形势。例如,安全协议在规模上不断复杂化的趋势为协议的安全性分析提出了很大的挑战。这种协议通常由许多较小的协议复合而成,但其安全性却不能简单地由各个较小协议的安全性自然地得到。原因在于敌手可将不同协议运行或同一协议不同运行中的消息相互交叉



中国科学院

使用,从而对协议的安全性构成威胁。一个通俗的例子是关于下棋的故事:象棋初学者 C 在网上同时与两位象棋高手 A 和 B 各下一盘棋:将 A 的招数用于对付 B,反过来又将 B 的招数用于对付 A。如果单独较量,两位高手必然都取胜。但 C 同时与 A、B 比赛,至少有一位高手是不能取胜的。在安全协议中,类似的威胁比这更为严重,因为我们甚至无法预测与一个协议同时运行的协议到底有多少。对这一问题的关注引出了对协议可复合性的研究。

下面对以上方法或问题的国际研究现状与发展趋势做简要综述。

3 国际研究进展与发展趋势

3.1 计算方法

安全协议分析中的计算方法源于上世纪 80 年代 Yao^[1]以及 Goldwasser 和 Micali^[2]等人的工作。这些工作为现代密码学的发展奠定了基础,促使了密码学由艺术向科学的转变。在这些工作的基础上,人们构造了一大批可证明安全的密码方案,包括各种加密方案、签名方案、零知识证明方案以及比特承诺方案等,为安全协议的构造奠定了坚实的基础。

然而,为了追求理论上的可证明性,通常需要付出较大的代价。一般来说,理论上可证明安全的协议构造极为复杂,运行效率低,很难在实际中使用。1995 年, Bellare 和 Rogaway 发现,假设存在随机应答器(Random Oracle, RO),那么许多可证明安全方案的效率将大大提高。这种模型被称为 RO 模型。相应地,将不使用随机应答器的模型称为标准模型。与一般应答器相比,随机应答器保持了对不同询问的随机应答,以及对相同询问的一致应答。但由于随机应答器是一个理想的“函数”,一个在 RO 模型中被证明安全的方案,在实际应用中一般使用一

个哈希函数来代替。尽管对 RO 模型下可证明的安全性还存在不同意见,但是一个不争的事实是,一般在 RO 模型下证明安全的方案,很少有实质性的攻击存在。况且这样的方案一般要比在标准模型下安全的类似方案效率高很多,由于它在协议安全性和协议效率之间进行了平衡,因此满足了实际应用的需求。

严格来说,计算方法最初主要用于对密码原语安全性的证明,要采用类似的方法分析协议的安全性,还必须建立适当的模型对协议及其安全性进行模拟。

1993 年, Bellare 和 Rogaway 提出了认证和密钥建立协议的一种安全模型,将计算方法用于对协议安全性的证明中,被称为 BR 模型。在 BR 模型中协议的交互过程被定义为敌手和应答器之间的对话,认证性是通过对话匹配来定义的,而保密性被定义为敌手“猜测”秘密的优势是可忽略的。

BR 模型的不足之处是可重用性差。1998 年, Bellare 等人采用模拟的思想提出一种可重用的 BCK 模型,其中采用了模块化设计。其主要思路是:将协议的设计与分析分为两个阶段,第一阶段,在理想认证环境下设计并证明协议;第二阶段,应用一个特定的认证子将协议转换为现实协议。以上两个阶段是相互独立的,因此每个阶段都可以被重用,以便由不同风格的认证方案得到不同的安全协议。

2001 年, Canetti 和 Krawczyk 在 BR 模型与 BCK 模型的基础上提出另一种模型,被称为 CK 模型。在 CK 模型中,对协议安全性的定义采用了与 BR 模型类似的不可区分性,但敌手模型采用了 BCK 中的定义,从而同时发挥了 BR 模型和 BCK 模型的优点。

2007 年, LaMacchia, Lauter 以及 Anton

Mityagin 等人对 CK 模型进行了扩展,进一步扩充了敌手对协议临时状态的获取机制,增强了对敌手的建模能力,使其可更灵活地建模各种攻击。

在这些模型的支持下,采用计算方法对安全协议进行分析成为一个活跃的研究课题。

3.2 形式化方法

形式化方法由来已久,甚至可以说,正是对形式化理论的研究促使了计算机的产生,但将形式化方法应用于安全协议分析的历史并不长。1978 年,Needham 和 Schroeder 对 Needham-Schroeder 协议^[3]的安全性行了简要分析,其中对敌手的能力进行了一定的抽象与假设。一般认为,该文献蕴含了一定的形式化分析思想。1981 年,Dolev 和 Yao^[4]首次明确提出了用形式化方法分析安全协议的思想,并给出一种协议形式化分析模型,即 Dolev-Yao 模型(简称 DY 模型)。DY 模型开启了安全协议形式化分析的先河,并为随后大量出现的协议形式化分析奠定了基础,几乎成为形式化分析的代名词。

近年来,人们针对安全协议分析提出了许多形式化方法^[5,6]。包括基于逻辑的方法、基于进程代数的方法以及基于定理证明的方法等。

上世纪 80 年代末 90 年代初,BAN^[7]逻辑的提出掀起了基于逻辑方法研究安全协议的高潮,成为形式化分析安全协议的一个里程碑。BAN 逻辑将体现信念的认知模态逻辑用于安全协议的分析,其中协议主体的信念被描述为一组公式,然后利用一组推理规则可从原有的信念中得到新的信念。BAN 逻辑的出现大大激发了应用形式化方法分析安全协议的兴趣,沿着这一方向,许多逻辑被构造了出来,其中大多是 BAN 逻辑的变种,目的是弥补 BAN 逻辑的不足。如,

GNV 逻辑在 BAN 逻辑中加入了新的元素,扩展了逻辑的应用范围;AT 逻辑和 SVO 逻辑给出了逻辑语义,保证了逻辑可靠性等等。在 BAN 之后,许多在计算机科学中已存在的形式化的方法,逐渐被用于对安全协议的分析上。因此,上个世纪 90 年代起,安全协议的形式化分析研究出现了空前的繁荣景象。

在基于进程代数的方法中,Gavin Lowe 成功地应用进程代数的模型检测工具发现 Needham-Schroeder 协议的一个漏洞。这个结果使人们看到了进程代数和模型检测在安全协议分析中的潜在的重要作用。1997 年,Abadi 等人基于另一种进程代数——Milner 的并发通信系统(CCS)及 Pi 演算,通过加入密码原语算子提出一种专门用于分析安全协议的进程代数 Spi 演算。2001 年,Abadi 等人又在 Spi 演算的基础上提出一种应用 Pi 演算(简称 Api),它通过在 Spi 演算的基础上加入等式理论,使得其对各种不同密码原语的建模更为灵活。

在基于定理证明的方法中,最具代表性的有:Paulson 的归纳证明法;Thayer Fábrega、Herzog 和 Guttman 等人提出的串空间模型(Strand Space)。定理证明的方法可以通过定理证明器辅助完成证明过程,如归纳法采用了 Isabelle 作为辅助工具,采用归纳的方法进行一步步推理,完成安全协议的安全性证明。串空间是用图的形式表达协议的执行过程。协议的一个丛就是协议的一个并发运行,协议的安全性质通过所有丛保持的性质来刻画。

纯粹的安全协议形式化分析方法在上世纪 90 年代达到繁荣阶段,本世纪以来,对形式化分析方法的研究一直没有停止,但向着更为深入的方向发展,这就是计算可靠的形式化方法。



中国科学院

3.3 计算可靠的形式化方法

2000年,Abadi和Rogaway在文献^[8]中首先给出了一种计算可靠的形式化方法,通常称其为AR逻辑。AR逻辑的主要目的是调和计算方法与形式化方法,其主要思想是:为协议消息提供两种模型,一种形式化模型,一种是计算模型,然后证明,在形式化模型下等价的消息在计算模型下是不可区分的。其中消息的等价是在形式化模型下由一定的规则定义的,而不可区分性是密码学中常用的概念。2004年,Micciancio和Warinschi进一步在给定条件下证明了AR逻辑的完备性,即如果使用充分强的加密方案,任何两个表达式计算等价当且仅当它们可以在逻辑下等价。AR逻辑的最大的意义在于为安全协议的分析开启了一个新的方向,提供了一种新的思路,但AR逻辑本身对安全协议的建模能力有限,它只能建模被动攻击下的安全性,即,敌手只是被动地窃听协议中传输的消息。2004年,Micciancio和Warinschi给出了主动攻击下的协议安全性证明的方法,将具有主动敌手的、简洁的逻辑转换到标准计算情形下。

大体来说,研究计算可靠性的方法可分为间接方法和直接方法。间接方法包括基于映射的方法和基于模拟的方法。基于映射的方法以Abadi、Micciancio^[8,9]等为代表,通常为协议的消息或行为迹建立一种从形式化模型到计算模型的映射,进而证明在形式化模型下成立的属性在计算模型下也成立,从而保持协议形式化分析的计算可靠性。基于模拟的方法以Canetti、Backes等人^[10,11]为代表,通常用交互式图灵机(ITM)或IO自动机建模协议各要素,将协议的属性用一种理想功能来体现,然后证明协议能够模拟理想功能。直接证明方法目前也包括两类,即基于逻辑的方法和基于Game序列的方法。基于

逻辑的方法以Impagliazzo、Kapron等人^[12,13]为代表,该方法直接对不可区分性作符号化抽象,采用逻辑公理的形式进行推理,以证明协议的安全性。基于Game序列的方法以Blanchet等人^[14]为代表,它直接将加密方案及签名方案中常用的Game序列方法形式化,通过等价替换完成一系列Game之间的归约,最终证明协议的安全性。

3.4 可复合安全协议分析

在协议的可复合性方面,Canetti在CK模型的基础上,提出了一种通用可复合(Universally Composable, UC)框架^[10]用于安全协议分析。该框架的基本要素是概率图灵机,其突出的特点就是它可提供通用可复合性保证,即,一个协议在独立运行情况下能实现其规范并可以被推广为,不管其周围网络中有什么样的活动,其规范照样可以被实现。在UC框架中,对协议安全性的刻画由现实协议与理想协议之间的模拟来完成。Backes, Pfitzmann和Waidner等人^[11]提出另一种满足协议可复合性的方法(BPW方法)。该方法采用交互式系统描述协议,系统的状态用数据库记录。针对DY模型可构造一种理想系统,其理想密码库可对用户提供抽象的密码操作。针对计算模型可构造实际系统,其实际密码库提供的命令与理想密码库相同,但包含有对实际密码的存储及具体的密码操作。最后证明存在一个模拟子,使得理想系统可模拟实际系统。模拟方法的使用使得BPW方法与UC方法在协议可复合性方面具有类似的思想。Mitchell通过在进程代数中加入概率对安全协议进行建模,其中,上下文的使用蕴含了一定的协议复合思想,但其安全性证明过程主要采用了计算的方法,且在该模型中概率的加入增加了协议分析的复杂性。Datta等人提出的PCL逻辑可在一定程度上描述协议的顺序或并行复

合,但这种复合不够通用,原因在于它仅考虑了复合对象的因素,而未考虑任意环境因素。最近,Canetti^[15]为了采用符号化方法分析安全协议,在 UC 框架的基础上给出了一种通用可复合的符号化分析方案(UCSA),但其方案首先需要在计算模型下对协议进行建模,然后再转换到符号化模型下进行分析,这一点对协议分析者提出了更高的要求。可见在协议的可复合性方面还有许多工作要做。

3.5 发展趋势

从安全协议分析的发展趋势来看,当前和今后一段时间的研究将呈现以下特点:

(1)安全协议的形式化分析是该领域的一个长期目标。在人类文明的发展过程中,工具始终是文明发展的标志。农业革命中手工工具的出现延伸了人的双手,工业革命中机械化工具的发展延伸了人的体力,而信息革命中自动化工具的发展所延伸的将是人类的思维。从这个意义上说,自动化是安全协议分析的终极目标。在计算机领域,形式化是自动化的必由之路。因此,安全协议的形式化分析以及安全协议自动分析工具的研制将是该领域的一个长期目标。

(2)建立合适的安全模型,扩大安全协议分析范围是今后一段时间计算方法的主要方向。在计算方法中,可证明安全的思想已相对成熟,但要将这种思想灵活地应用于安全协议,必须建立合适的安全模型。当前一些模型主要针对认证和密钥建立协议,且对敌手的建模能力有限。因此,建立合适的安全模型,扩大安全协议分析范围是今后一段时间计算方法的主要方向。

(3)计算可靠性和通用可复合性作为本领域研究热点的状况仍将继续。在当前,计算可靠性和通用可复合性的研究是安全协议分析的研究热点,但其研究结果还远远没

有达到现实需求。以计算可靠性为例,当前的研究还主要体现在理论形成阶段,对具体协议的分析结果还比较缺乏。主要原因在于,当前的研究主要注重结果的正确性,在实际应用中对具体协议的建模能力有限。另外,在计算可靠性研究方面,直接证明方法近年刚刚兴起,还需要进一步发展与完善。在可复合性方面,安全协议不断复杂化的发展趋势决定了协议可复合性研究仍将是今后一段时间的研究热点。当前在可复合性研究方面存在的主要问题是分析模型过于复杂,需要进一步简化,与形式化方法相结合。

(4)信息业务的多样化呼唤对安全属性更多的分析。当前,对安全协议的分析主要集中在保密性与认证性上。事实上,协议的安全性远远不止这些。例如在电子商务中,公平性是一种非常重要的安全属性,但目前对公平性的分析手段极为有限,形式化的分析方法更为缺乏。在电子投票协议中,匿名性是一种很典型的安全属性,但对匿名性的分析也很少受到关注。更有甚者,可用性作为一种重要的安全属性已经受到人们的长期的广泛关注,但至今缺乏有效的形式化分析方法。

(5)代码级的安全协议分析将成为安全协议分析的又一热门方向。当前,很少有代码级的安全协议分析,但从发展的角度来看,代码级的分析将是安全协议分析的一个必然方向。任何理论问题要发挥现实作用,必须落实在实现上,安全协议也不例外。从应用的角度来说,安全协议最终的表现形式是程序代码。一种经过理论分析被证明安全的协议,很可能在实现过程中引入新的安全问题。要防止这类安全问题的出现,必须在代码级研究协议的安全性。在这一点上,软件正确性分析的历史就是一个很好的例证。不仅如此,软件工程以及软件形式化验证的



中国科学院

一些方法可以为代码级的安全协议分析提供很好的借鉴。

4 国内研究现状与对策建议

4.1 国内研究现状

在安全协议分析的研究方面,值得一提的是,我国科学家姚期智先生在上世纪 80 年代所取得的成就无论在计算方法^[9]还是在形式化方法^[10]上都对安全协议的分析起到了奠基性的作用并产生了持久的影响。在安全协议分析的计算方法上,近年来,我国学者取得了一批具有国际影响的研究成果,如在密码交换协议及零知识协议的证明方面达到了国际先进水平^[11],但在安全模型方面还缺少创造性成果。在形式化方法上,目前与国外研究差距较大,缺乏原创性的、具有国际影响力的成果,处于引进、吸收、消化、应用、改进阶段。在计算可靠性及协议可复合性方面还处于起步阶段。总体来说,我国在安全协议的研究方面偏重于计算方法,而在形式化方法、形式化方法的计算可靠性以及协议可复合性等方面差距明显,相关人才资源匮乏,亟需加强。

4.2 建议与对策

为了尽快缩小我国当前在安全协议研究方面的差距,提出以下建议与对策:

(1)从学科建设的角度,加强安全协议的专业地位。安全协议分析是一个典型的交叉学科。广义上,它是数学与信息安全的交叉。具体上说,它需要数学、逻辑学、密码学、计算机科学等方面的专业知识。目前大部分机构并没有将安全协议作为一个专业的专业来对待,许多从事安全协议分析的研究人员来自于各种不同的专业。例如,在安全协议分析方面一个较为普遍的现象是,做形式化方向的不熟悉密码学,而做密码学方向的又不熟悉形式化。加上形式化方法和密码学本身都是需要潜心研究的学科,要掌握它

们不可能一蹴而就。故此,建议在部分院校设立独立的安全协议专业,将数学、逻辑学、密码学、计算机科学等专业中与安全协议密切相关的内容整合起来,形成安全协议专业基础,再加上安全协议本身的一些理论构成安全协议专业的主要内容。同时组织一批力量,出版安全协议专业配套教材,以配合安全协议专业的设立。从而,在学科建设上为安全协议的发展奠定基础。

(2)从标准制定的角度,规范安全协议的使用标准。实践证明,标准的制定是促进相关科学研究的重要推动力。以安全相关标准为例,国外在 1983 年就发布了 TCSEC 标准,这一标准的发布对一定安全级别的信息系统提出了许多强制性安全要求,促进了一大批力量投入相关研究。而我国与其类似的标准 GB17859 于 1999 年发布,比国外晚了很多年,这也是我国在信息安全某些领域研究滞后的原因之一。近年来,我国在标准的制定方面与国外类似标准的滞后周期明显缩短。如 1999 年国际通用安全评价标准 CC 出台,我国与此类似的标准 GB/T 18336 也于随后的 2001 年颁布,信息安全系统等级评定工作也在近几年全面展开。这些都为我国信息安全的发展起到了推动作用。

由此建议,在信息系统安全标准的基础上进一步制定针对安全协议的国家标准,设定一定安全等级及等级标准。一定等级标准的安全协议必须通过相应的安全性分析与验证之后才能认可。同时加强政策的制定,强制要求一定安全级别的机构在网络通信中必须使用相应级别的安全协议。这样不仅可以刺激对协议安全性的研究,而且也从客观上加强国内各机构重要信息的安全性,减少不必要的损失。

(3)从项目引导的角度,加强对安全协议的支持力度。项目对于相关科研具有一定



的引导作用。如果没有一定的项目支撑,相关研究将难以持久。在发挥项目引导作用时对一些研究薄弱的科研领域必须给予一定的政策倾斜,否则将会形成恶性循环,使得薄弱环节更为薄弱。以安全协议的研究为例,目前国内研究与国外差距明显,相关科研成果较少,这也为相关科研人员申请项目造成不利影响,而没有项目的支撑将进一步导致该领域研究力量的流失,从而形成恶性循环。

为了充分发挥项目的引导作用,建议在国家各种基金项目中对安全协议分析研究在政策上予以重点支持,提高资助比例与资助力度。在支持的重点方向上,以未来的发展趋势为导向,尤其是一些当前发展尚不成熟、但极具发展潜力的方向。抓住机遇,鼓励原始创新,变被动为主动,提高国际影响力。另外,在资助规模上形成梯次配置,从重点项目、大型项目到一般项目、小型项目都应当有一定的扶持力度,这样既可促进安全协议分析研究在当前的发展,也可吸引更多的年轻人投入到该领域中来,为该领域的发展储备人才,改变目前安全协议分析领域人才匮乏的状况。

(4)从人才培养的角度,加强安全协议的国际交流。在人才培养方面,以上三方面均可从不同角度间接调整人才资源配置,吸引相关研究人员投入到协议分析领域。除此之外,还需要采取“引进来”、“走出去”的策略,加强国际交流,提升我国在安全协议方面的国际竞争力。由当前国际发展现状来看,在安全协议分析的研究上,大部分成果集中在欧美国家。例如,美国在安全协议分析的各方面均走在前列,除此之外,以色列在密码学、英国在形式化方法、法国在计算可靠性方面均有突出的成果。通过与国外相关机构加强学术交流与合作、把国外相关领

域人才请进来,或者选派有潜力的研究人员出国访问交流等方式加速高端人才的培养,将有利于缩小我国与国外研究的差距。

主要参考文献

- 1 Yao A C. Theory and application of trapdoor functions. In Proc. 23rd IEEE Symp. on Foundations of Comp. Science, Chicago, 1982: 80-91.
- 2 Goldwasser S, Micali S. Probabilistic encryption. JCSS, 1984, 28(2):270-299.
- 3 Needham R M and Schroeder M D. "Using encryption for authentication in large networks of computers," Communications of the ACM, 1978, 21(12): 993-999.
- 4 Dolev D, Yao A C. On the security of public-key protocols. IEEE Transactions on Information Theory, 1983, 30(2):198-208.
- 5 薛锐,冯登国. 安全协议的形式化分析技术与方法. 计算机学报, 2006, 29(1): 1-20.
- 6 薛锐. 安全协议的形式化分析方法及其发展现状. 中国密码学发展报告 2008. 北京: 电子工业出版社, 2009:103-138.
- 7 Burrows M, Abadi M, Needham R. "A logic of authentication," ACM Transactions on Computer Systems, 1990, 8(1): 18-36.
- 8 Abadi M, Rogaway P. "Reconciling two views of cryptography (the computational soundness of formal encryption)," in TCS '00: Proceedings of the International Conference IFIP on Theoretical Computer Science, Exploring New Frontiers of Theoretical Informatics. London, UK: Springer-Verlag, 2000: 3-22.
- 9 Micciancio D, Warinschi B. Soundness of formal encryption in the presence of active adversaries. In Moni Naor, editor, Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA: Proceedings, volume

- 2951 of Lecture Notes in Computer Science, Springer, 2004: 133-151.
- 10 Canetti R. Universally composable security: A new paradigm for cryptographic protocols. In 42th IEEE Symposium on Foundations of Computers Science, 2001: 136-145.
- 11 Backes M, Pfitzmann B, Waidner M. A composable cryptographic library with nested operations (extended abstract). In Proceedings, 10th ACM conference on computer and communications security (CCS), 2003.
- 12 Impagliazzo R, Kapron B M. Logics for reasoning about cryptographic constructions. J. Comput. Syst. Sci., 2006, 72(2):286-320.
- 13 Barthe G, Daubignard M, Kapron B et al. Computational indistinguishability logic. In Proceedings of the 17th ACM conference on Computer and communications security, CCS '10, ACM, New York, USA, 2010: 375-386.
- 14 Blanchet B, Pointcheval D. Automated security proofs with sequences of games. In Cynthia Dwork, editor, CRYPTO, volume 4 117 of Lecture Notes in Computer Science. Springer, 2006:537-554.
- 15 Canetti R, Herzog J. Universally composable symbolic security analysis. Journal of Cryptology, 2011, 24(1):83-147.
- 16 中国科学技术协会, 中国密码学学会. 2009-2010 密码学学科发展报告. 北京: 中国科学技术出版社, 2010.

Present Status and Trends of Researches on Analyses of Security Protocols

Xue Rui Lei Xinfeng

(State Key Laboratory of Information Security, Institute of Software, CAS 100190 Beijing)

Abstract Information assurance is faced with great challenges in the information society. As the soul of information assurance in networks, security protocols play an important role. As a result, research on security analyses of security protocols becomes a dominant problem. By surveying on the present status and developments of the analyses of security protocols, we conclude that, as a whole, there need much endeavors to be made in China to catch the international researched in this area. It is urgent for us to strengthen in academic research and practical developments. Based on this view, some countermeasures and suggestions are provided to promote the researches in China.

Keywords security protocol, cryptography, formal method, research status, trends

薛 锐 中国科学院软件研究所信息安全国家重点实验室研究员, 博士生导师。于北京师范大学数学系分别获得学士、硕士和博士学位; 曾在德国 Passau 大学、美国普渡大学和美国伊利诺伊(UIUC)大学计算机科学系访问研究。多年来主要从事数理逻辑、密码学与安全协议等方面的研究工作。曾参加多项国家重大基础研究项目(“973”); 主持完成多项国家“863”项目和多项国家自然科学基金等项目。在国内外刊物、国际国内会议上发表近百篇论文。领导开发完成 AVSP 以及 ASM-SPV 等安全协议验证工具。E-mail: ruixue.cn@gmail.com